UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,121	01/26/2001	Stefan Johansson	15292.5	7000

22913 7590 12/28/2007
WORKMAN NYDEGGER
60 EAST SOUTH TEMPLE
1000 EAGLE GATE TOWER
SALT LAKE CITY, UT 84111

EXAMINER	
MOORE, IAN N	
ART UNIT	PAPER NUMBER
2616	
MAIL DATE	DELIVERY MODE
12/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/771,121	**Applicant(s)** JOHANSSON ET AL.	
	Examiner Ian N. Moore	**Art Unit** 2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 November 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. *09/684,057*.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *6-27-2007*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 13 recites, "**all** the packet data" in line 21. It is unclear whether "all the packets data" includes the packet data that is transmitted in "transmitting from an originator…the originator's own network address" lines 7-8. Note that the data packet having the address does not make the differentially since all data packet that is transmitted over the wireless mobile communication has the address. "**All** the packet data" recited in line 21 cannot be "**all**" if "some" is already being transmitted in lines 7-8.

Claim 1 is also rejection for the same reason as set forth above in claim x.

Claims 2-24 and 14-22 are also rejected since they are depended upon rejected claims 1 and 2 as set forth above.

Double Patenting

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference

claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1 and 13 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 and 13 of copending Application No. 09/771,120 (US 2001/0015977A1) (hereinafter refers to Johansson'120) in view of Oka (US006091945A).

Regarding claim 1 of the instant application, Johansson'120 discloses a method at a wireless mobile communication station for enabling the wireless mobile communication station to control when pushed packet data from an originator is received by the wireless mobile communication station, the station being operatively associated with a wireless communication network providing packet data transferring services, the method comprising the acts of: (see Johansson'120 claim 1, line 1-5),

receiving at the wireless mobile communication station a network address of an originator of packet data that is attempting to push the packet data to the wireless mobile communication station (see Johansson'120 claim 1, line 9-13);

determining, at the wireless mobile communication station, if the received network address (see Johansson'120 claim 1, lines 14-17);

verifying, at the wireless mobile communication station, the identity of the originator (see Johansson'120 claim 1, lines 14-17); and

after verifying the identity of the originator, the wireless mobile communication station using the received network address of the originator to establishing establish a packet data session with the originator and only after the identity of the originator is verified as being authentic, such that all the packet data is transmitted from the originator only after the wireless mobile communication station determination (see Johansson'120 claim 1, line 18-24),

thereby ascertaining that pushed packet data is received by the wireless mobile communication station only from one or more predefined originators (see Johansson'120 claim 1, line 25-27).

Johansson'120 does not explicitly disclose "matches a predefined network address of the originator that is included in a set of one or more predefined network addresses stored by the communication station, the set of one or more predefined network addresses corresponding to one or more predefined originators of packet data, when the received network address of the originator matches one or more of the predefined network addresses stored by the communication station, that the received network address is included in the set of one or more predefined network addresses stored by the communication station".

However, Oka teaches determining at the wireless mobile communication station if the received network address matches a predefined network address of the originator (see FIG. 3, S22-S24; see FIG. 4, S32-34; determining/checking at Mobile Station (callee) if the received fixed ID, variable ID and telephone number of caller mobile station) is included in a set of one or more predefined network addresses stored by the wireless mobile communication station (see

FIG. 2, Mobile station 1 memorizes IDs and telephone numbers (i.e. group/set of network addresses) of other mobile stations, and comparing unit 111 compares the received IDs and numbers with stored IDs and number; see FIG. 3-4, S23,S24,S33,S34; see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40), the set of one or more predefined network address corresponding to one or more predefined originators of data (see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40; the memorized IDs and numbers relate/correspond to other mobile stations (caller));

verifying, at the wireless mobile communication station, the identify of the originator when the received network address of the originator matches one or more of the predefined network address stored by the wireless mobile communication station (see FIG. 3, S22-S24; see FIG. 4, S32-34; verifying/authenticating at the callee mobile station the identify ID of the caller when received network ID/address of the caller recognized/matches the memorized network IDs/numbers of caller mobile stations; see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40);

after verifying the identify of the originator (see FIG. 3, S23-27, S17; see FIG. 4, S33-S38; after verifying/authenticating the ID of the caller mobile station), the wireless mobile communication station using the received network address of the originator to establish a session with the originator at the wireless mobile communication station only after the identity of the originator is verified as being authentic (see FIG. 3, S23-27,S17; see FIG. 4, S33-S38; establishing communication with the caller mobile station at the callee mobile station after the verifying that the caller station is authentic; see col. 6, line 44 to col. 7, line 10, 30-40; see col. 8, line 3-11) such that all the data is transmitted from the originator (see FIG. 3, S17 and see FIG.

4, S38; when communication is established all the data transmitted from the caller station and received by the callee mobile station; see col. 7, line 5-11; see col. 8, line 5-11) only after the wireless communication station determines that the received network address is included in the set of one or more predefined network address stored by the wireless mobile communication station (see FIG. 3-4, S17/S38 (establishing communication step) at the callee mobile station occurs only after S22-24/S33-S34 (determining and authentication/verification steps) which determine by comparing the received caller IDs and number with the memorized IDs and number by the callee mobile station; see col. 6, line 44 to col. 7, line 10, 30-40; see col. 8, line 3-11).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide "matches a predefined network address of the originator that is included in a set of one or more predefined network addresses stored by the communication station, the set of one or more predefined network addresses corresponding to one or more predefined originators of packet data, when the received network address of the originator matches one or more of the predefined network addresses stored by the communication station, that the received network address is included in the set of one or more predefined network addresses stored by the communication station", as taught by Oka in the system of Andersson, so that it would provide improved authentication method in a radio communication system; see Oka col. 3, line 50-55.

Regarding claim 13 of the instant application, Johansson'120 discloses a method of a system which includes a wireless mobile communication station and an originator of information for enabling the wireless mobile communication station to control when pushed packet data from an originator is received by the wireless mobile communication station, the wireless mobile communication station being operatively associated with a wireless communication network providing packet data transferring services, the method comprising the acts of (see Johansson'120 claim 13, lines 1-6):

transmitting, from an originator that is attempting to push packet data to the wireless mobile communication station, the originator's own network address (see Johansson'120 claim 13, liens 7-12);

determining, at the wireless mobile communication station, if the received network address (see Johansson'120 claim 13, lines 13-22);

verifying, at the wireless mobile communication station, the identity of the originator, by the wireless mobile communication station (see Johansson'120 claim 13, line 17-22); and

after verifying the identity of the originator, the wireless mobile communication station using the received network address of the originator to establishing establish a packet data session with the originator, and only after the originator is determined by the wireless mobile communication station to be authentic such that all the packet data is transmitted from the originator only after the wireless mobile communication station determination (see Johansson'120 claim 13, line 23-31)

thereby ascertaining that pushed packet data only is received by the wireless mobile communication station only from one or more predefined originators (see Johansson'120 claim 13, line 30-33).

Johansson'120 does not explicitly disclose "matches a predefined network address of the originator that is included in a set of one or more predefined network addresses stored by the communication station, the set of one or more predefined network addresses corresponding to one or more predefined originators of packet data, when the received network address of the originator matches one or more of the predefined network addresses stored by the communication station, that the received network address is included in the set of one or more predefined network addresses stored by the communication station".

However, Oka teaches determining at the wireless mobile communication station if the received network address matches a predefined network address of the originator (see FIG. 3, S22-S24; see FIG. 4, S32-34; determining/checking at Mobile Station (callee) if the received fixed ID, variable ID and telephone number of caller mobile station) is included in a set of one or more predefined network addresses stored by the wireless mobile communication station (see FIG. 2, Mobile station 1 memorizes IDs and telephone numbers (i.e. group/set of network addresses) of other mobile stations, and comparing unit 111 compares the received IDs and numbers with stored IDs and number; see FIG. 3-4, S23,S24,S33,S34; see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40), the set of one or more predefined network address corresponding to one or more predefined originators of data (see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40; the memorized IDs and numbers relate/correspond to other mobile stations (caller));

verifying, at the wireless mobile communication station, the identify of the originator when the received network address of the originator matches one or more of the predefined network address stored by the wireless mobile communication station (see FIG. 3, S22-S24; see FIG. 4, S32-34; verifying/authenticating at the callee mobile station the identify ID of the caller when received network ID/address of the caller recognized/matches the memorized network

IDs/numbers of caller mobile stations; see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40);

after verifying the identify of the originator (see FIG. 3, S23-27,S17; see FIG. 4, S33-S38; after verifying/authenticating the ID of the caller mobile station), the wireless mobile communication station using the received network address of the originator to establish a session with the originator at the wireless mobile communication station only after the identity of the originator is verified as being authentic (see FIG. 3, S23-27,S17; see FIG. 4, S33-S38; establishing communication with the caller mobile station at the callee mobile station after the verifying that the caller station is authentic; see col. 6, line 44 to col. 7, line 10, 30-40; see col. 8, line 3-11) such that all the data is transmitted from the originator (see FIG. 3, S17 and see FIG. 4, S38; when communication is established all the data transmitted from the caller station and received by the callee mobile station; see col. 7, line 5-11; see col. 8, line 5-11) only after the wireless communication station determines that the received network address is included in the set of one or more predefined network address stored by the wireless mobile communication station (see FIG. 3-4,.S17/S38 (establishing communication step) at the callee mobile station occurs only after S22-24/S33-S34 (determining and authentication/verification steps) which determine by comparing the received caller IDs and number with the memorized IDs and number by the callee mobile station; see col. 6, line 44 to col. 7, line 10, 30-40; see col. 8, line 3-11).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide "matches a predefined network address of the originator that is included in a set of one or more predefined network addresses stored by the communication station, the set of one or more predefined network addresses corresponding to one or more predefined originators of packet data, when the received network address of the originator matches one or more of the predefined network addresses stored by the communication station, that the received network address is included in the set of one or more predefined network addresses stored by the communication station", as taught by Oka in the system of Andersson, so that it would provide improved authentication method in a radio communication system; see Oka col. 3, line 50-55.

Moreover, the doctrine of double patenting seeks to prevent the unjustified extension of patent exclusivity beyond the term of a patent.

This is a provisional obviousness-type double patenting rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 5-7, 11-13, 17-19, 23 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andersson (US006047194A) in view of Oka (US006091945A).

Regarding Claim 1, Andersson discloses a method at a wireless mobile communication station (see FIG. 1, Mobile terminal 14) for enabling the wireless mobile communication station to control when pushed packet data from an originator (see FIG. 1, from Internet Host 12) is received by the wireless mobile communication station, the station being operatively associated with a wireless communication network providing packet data transferring services (see col. 3, line 40-47; packet switching network), the method comprising the acts of:

receiving at the wireless mobile communication station a network address of an originator of packet data that is attempting to push the packet data to the mobile communication station (see FIG. 2, 114; see FIG. 4, step 168; see col. 5, line 65 to col. 6, line 14; see col. 7, line 40-65; see col. 8, line 45-56; see col. 10, line 57-57; mobile terminal receives an SMS message with in identifier (i.e. Origination Address (OA) according to GSM's SMS standard) of the origination source/host that is trying to send packet data; note that a SMS message is a request/query/signaling packet to the mobile station to determine the mobile station permission for an end-to-end transmission);

determining at the wireless mobile communication station if the received network address matches a predefined network address of the originator stored the wireless mobile communication station (see FIG. 4, step 172; see col. 6, line 4-10; see col. 7, line 60 to col. 8, line 2, 59-65; see col. 9, line 32-35; see col. 10, line 50-56; mobile terminal determines the received identifier/OA of the origination source associates/matches with stored/predetermined identifier/OA), the predefined network address corresponding to one predefined originator of packet data (see FIG. 4, step 172; see col. 6, line 4-10; see col. 7, line 60 to col. 8, line 2, 59-65; see col. 9, line 32-35; see col. 10, line 50-56; the stored network identifier/address corresponds/relates to the origination source);

verifying at the wireless mobile communication station the identity of the originator when the received network address of the originator matches one predefined network addresses stored by the wireless mobile communication station (see FIG. 4, step 174; see col. 6, line 5-14; see col.

8, line 3-65; see col. 9, line 35-40; mobile user verifies/authenticates/permits/selects the identify of the origination sources when received identifier/address of the origination source corresponds/matches the stored identifier/addresses (i.e. user can only verify/authenticate/permit/select "the identifier/address" if the received identifier/address matches/corresponds with stored/predetermined identifiers/addresses));

after verifying the identify of the originator (see col. 6, line 1-12; see col. 8, line 28-65; after verifying/authenticating/permitting identify of the origination source), the wireless mobile communication station using the received network address of the originator to establish a packet data session with the originator only after the identity of the originator is verified (see FIG. 4, step 176; see col. 6, line 10-14; see col. 8, line 10-14, 60-67; see col. 9, line 40-44; the mobile station using the OA of the origination source by initiating registration procedure in order to establish an end-to-end packet session/connection with the origination source only after the identify of the origination source is verified/authenticated/permitted), such that the packet data is transmitted from the originator (see FIG. 4, step 176; see col. 5, line 65 to col. 6, line 14; see col. 8, line 59 to col. 9, line 5; so that the packet data, which is not a SMS message request/query/signaling packet, is transmitted from the origination source to the mobile station via a registered end-to-end connection) only after the wireless mobile communication station determines that the received network address is included in the set of one or more predetermined network address stored by the wireless mobile station (see FIG. 4, step 168,172,174; only after the mobile station detects/determines that received identifier/address of the origination source corresponds/matches the stored/predefined identifiers/addresses by the mobile station and permitting/selecting accepted identifier/address of the origination source; see col. 8, line 21-44, 50 to col. 9, line 5),

thereby ascertaining that pushed packet data only is received by the wireless mobile communication station only from one or more predefined originators (see col. 8, line 10-14, 60-67; col. 8, line 65 to col. 9, line 6; thereby determining at the mobile station that the packet data is received only from verified/authenticated/permitted/selected origination source).

Andersson does not explicitly disclose "including in a set of one or more addresses and verified as being authentic" and "all".

However, Oka teaches determining at the wireless mobile communication station if the received network address matches a predefined network address of the originator (see FIG. 3, S22-S24; see FIG. 4, S32-34; determining/checking at Mobile Station (callee) if the received fixed ID, variable ID and telephone number of caller mobile station) is included in a set of one or more predefined network addresses stored by the wireless mobile communication station (see FIG. 2, Mobile station 1 memorizes IDs and telephone numbers (i.e. group/set of network addresses) of other mobile stations, and comparing unit 111 compares the received IDs and numbers with stored IDs and number; see FIG. 3-4, S23,S24,S33,S34; see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40), the set of one or more predefined network address corresponding to one or more predefined originators of data (see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40; the memorized IDs and numbers relate/correspond to other mobile stations (caller));

verifying, at the wireless mobile communication station, the identify of the originator when the received network address of the originator matches one or more of the predefined network address stored by the wireless mobile communication station (see FIG. 3, S22-S24; see FIG. 4, S32-34; verifying/authenticating at the callee mobile station the identify ID of the caller when received network ID/address of the caller recognized/matches the memorized network IDs/numbers of caller mobile stations; see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40);

after verifying the identify of the originator (see FIG. 3, S23-27, S17; see FIG. 4, S33-S38; after verifying/authenticating the ID of the caller mobile station), the wireless mobile communication station using the received network address of the originator to establish a session with the originator at the wireless mobile communication station only after the identity of the originator is verified as being authentic (see FIG. 3, S23-27,S17; see FIG. 4, S33-S38; establishing communication with the caller mobile station at the callee mobile station after the verifying that the caller station is authentic; see col. 6, line 44 to col. 7, line 10, 30-40; see col. 8, line 3-11) such that all the data is transmitted from the originator (see FIG. 3, S17 and see FIG. 4, S38; when communication is established all the data transmitted from the caller station and received by the callee mobile station; see col. 7, line 5-11; see col. 8, line 5-11) only after the wireless communication station determines that the received network address is included in the set of one or more predefined network address stored by the wireless mobile communication station (see FIG. 3-4, S17/S38 (establishing communication step) at the callee mobile station occurs only after S22-24/S33-S34 (determining and authentication/verification steps) which determine by comparing the received caller IDs and number with the memorized IDs and number by the callee mobile station; see col. 6, line 44 to col. 7, line 10, 30-40; see col. 8, line 3-11).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide "a portable device stores plurality of address and perform authentication", as taught by Oka in the system of Andersson, so that it would provide improved authentication method in a radio communication system; see Oka col. 3, line 50-55.

Regarding Claims 13 and 23, Andersson discloses a method of a system which includes a wireless mobile communication station (see FIG. 1, Mobile terminal 14) for enabling the wireless mobile communication station to control when pushed packet data from an originator (see FIG. 1, from Internet Host 12) is received by the wireless mobile communication station, the station being operatively associated with a wireless communication network providing packet data transferring services (see col. 3, line 40-47; packet switching network), the method comprising the acts of:

transmitting, from an originator (see FIG. 1, sending to Short Message Service-Center (SMS-C) 56) from an originator (see FIG. 1, Internet host 12) that is attempting to push packet data to the wireless mobile communication station (see col. 7, line 16-54; from the Internet host 12 that is trying/attempting to push/send the packet data to the mobile terminal), the originator's own network address (see col. 7, line 45-53; source IP address); see FIG. 2, 114; see FIG. 4, step 168; see col. 5, line 65 to col. 6, line 7; see col. 7, line 40-65; see col. 8, line 45-56; see col. 10, line 57-57; mobile terminal receives a transmitted SMS message with in identifier (i.e. Origination Address (OA) according to GSM's SMS standard) of the origination source/host that is trying to send packet data; note that a SMS message is a request/query/signaling packet to the mobile station to determine the mobile station permission for an end-to-end transmission);

determining if the received network address matches a predefined network address of the originator stored the wireless mobile communication station (see FIG. 4, step 172; see col. 6, line 4-10; see col. 7, line 60 to col. 8, line 2, 59-65; see col. 9, line 32-35; see col. 10, line 50-56; mobile terminal determines the received identifier/OA of the origination source associates/matches with stored/predetermined identifier/OA); the predefined network address corresponding to one predefined originator of packet data (see FIG. 4, step 172; see col. 6, line 4-10; see col. 7, line 60 to col. 8, line 2, 59-65; see col. 9, line 32-35; see col. 10, line 50-56; the stored network identifier/address corresponds/relates to the origination source);

- verifying the identity of the originator at the wireless mobile communication station when the received network address of the originator matches one predefined network addresses stored by the wireless mobile communication station (see FIG. 4, step 174; see col. 6, line 5-14; see col. 8, line 3-65; see col. 9, line 35-40; mobile user verifies/authenticates/permits/selects the identify of the origination sources if received identifier/address of the origination source corresponds/matches the stored identifier/addresses (i.e. user can only verify/authenticate/permit/select "the identifier/address" if the received identifier/address matches/corresponds with stored/predetermined identifiers/addresses));

after verifying the identify of the originator (see col. 6, line 1-12; see col. 8, line 28-65; after verifying/authenticating/permitting identify of the origination source), the wireless mobile communication station using the received network address of the originator to establish a packet data session with the originator at the wireless mobile communication station only after the identity of the originator is verified (see FIG. 4, step 176; see col. 6, line 10-14; see col. 8, line 10-14, 60-67; see col. 9, line 40-44; the mobile station using the OA of the origination source by initiating registration procedure in order to establish an end-to-end packet session/connection with the origination source only after the identify of the origination source is verified/authenticated/permitted) such that the packet data is transmitted from the originator (see FIG. 4, step 176; see col. 5, line 65 to col. 6, line 14; see col. 8, line 59 to col. 9, line 5; so that the packet data, which is not a SMS message request/query/signaling packet, is transmitted from the origination source to the mobile station via a registered end-to-end connection), only after determining that the received network address is included in the set of one or more predetermined network address stored by the wireless mobile station see FIG. 4, step 168,172,174; only after the mobile station detects/determines that received identifier/address of the origination source corresponds/matches the stored/predefined identifiers/addresses by the mobile station and permitting/selecting accepted identifier/address of the origination source; see col. 8, line 21-44, 50 to col. 9, line 5),

thereby ascertaining that pushed packet data only is received from one or more predefined originators (see col. 8, line 10-14, 60-67; col. 8, line 65 to col. 9, line 6; thereby determining that the packet data is received only from verified/selected origination source).

Andersson does not explicitly disclose "including in a set of one or more addresses and verified as being authentic" and "all".

However, Oka teaches determining at the wireless mobile communication station if the received network address matches a predefined network address of the originator (see FIG. 3, S22-S24; see FIG. 4, S32-34; determining/checking at Mobile Station (callee) if the received fixed ID, variable ID and telephone number of caller mobile station) is included in a set of one or more predefined network addresses stored by the wireless mobile communication station (see

FIG. 2, Mobile station 1 memorizes IDs and telephone numbers (i.e. group/set of network addresses) of other mobile stations, and comparing unit 111 compares the received IDs and numbers with stored IDs and number; see FIG. 3-4, S23,S24,S33,S34; see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40), the set of one or more predefined network address corresponding to one or more predefined originators of data (see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40; the memorized IDs and numbers relate/correspond to other mobile stations (caller));

verifying, at the wireless mobile communication station, the identify of the originator when the received network address of the originator matches one or more of the predefined network address stored by the wireless mobile communication station (see FIG. 3, S22-S24; see FIG. 4, S32-34; verifying/authenticating at the callee mobile station the identify ID of the caller when received network ID/address of the caller recognized/matches the memorized network IDs/numbers of caller mobile stations; see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40);

after verifying the identify of the originator (see FIG. 3, S23-27,S17; see FIG. 4, S33-S38; after verifying/authenticating the ID of the caller mobile station), the wireless mobile communication station using the received network address of the originator to establish a session with the originator at the wireless mobile communication station only after the identity of the originator is verified as being authentic (see FIG. 3, S23-27,S17; see FIG. 4, S33-S38; establishing communication with the caller mobile station at the callee mobile station after the verifying that the caller station is authentic; see col. 6, line 44 to col. 7, line 10, 30-40; see col. 8, line 3-11) such that all the data is transmitted from the originator (see FIG. 3, S17 and see FIG.

4, S38; when communication is established all the data transmitted from the caller station and received by the callee mobile station; see col. 7, line 5-11; see col. 8, line 5-11) only after the wireless communication station determines that the received network address is included in the set of one or more predefined network address stored by the wireless mobile communication station (see FIG. 3-4, S17/S38 (establishing communication step) at the callee mobile station occurs only after S22-24/S33-S34 (determining and authentication/verification steps) which determine by comparing the received caller IDs and number with the memorized IDs and number by the callee mobile station; see col. 6, line 44 to col. 7, line 10, 30-40; see col. 8, line 3-11).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide "a portable device stores plurality of address and perform authentication" and "all", as taught by Oka in the system of Andersson, so that it would provide improved authentication method in a radio communication system; see Oka col. 3, line 50-55.

Regarding Claims 5 and 17, the combined system of Andersson and Oka discloses all limitation as set forth above in claim 1 and 13. Andersson further discloses wherein said network address of said receiving act is received in a short message (see col. 6, line 1-10; SMS), the short message being received from a short message service provided by said wireless communication network (see FIG. 1, Short Message service-center, SMS-C 56; see col. 5, line 60 to col. 6, line 10).

Regarding Claims 6 and 18, the combined system of Andersson and Oka discloses all limitation as set forth above in claim 1 and 13. Andersson further discloses establishing a packet data session using the originator network address (see col. 5, line 65 to col. 6, line 14; see col. 7, line 40-65; see col. 8, line 10-14,45-67; see col. 9, line 40-44; see col. 10, line 57-57).

Regarding Claims 7 and 19, the combined system of Andersson and Oka discloses all limitation as set forth above in claim 1 and 13. Andersson further discloses wherein said network address is an Internet Protocol address (see col. 7, line 40-35; IP address).

Regarding Claim 11, the combined system of Andersson and Oka discloses a computer-readable medium storing computer-executable components for causing a wireless communication station to perform the acts recited in claim 1 and 13 when the computer-executable components are run on microprocessor included by a wireless communication station (see Andersson FIG. 3, mobile terminal 14 contains processor and memory; see col. 8, line 14-32; see Moore FIG. 2-3, Memory 240/340, control circuit 206/315).

Regarding Claim 12, the combined system of Andersson and Oka a wireless communication station (see Andersson FIG. 3, mobile terminal 14; see Oka FIG. 2, mobile station 1) arranged to be operatively associated with a wireless communication network (see Andersson FIG. 1, mobile network) providing packet data transferring services, wherein the wireless communication station includes processing means (see Andersson FIG. 3, mobile terminal 14 contains processor; see Oka FIG. 2, control unit 101), memory means (see Andersson FIG. 3, mobile terminal 14 contains memory; see Oka FIG. 2, Memory means), interface circuitry means (see Andersson FIG. 3, Rx circuitry 142 with radio antenna interface; see Oka FIG. 2, transmission and reception circuit 102) and user interface means (see Andersson FIG. 3, Display 144 and selector 146) for performing the acts recited in claim 1 (see Andersson col. 8, line 14-32), thereby facilitating desired packet data to be pushed from an originator to the wireless communication station (see Andersson col. 15, line 16-42; thereby providing the subscriber to select desired/preferred packet data system provider to receive the packet data).

Regarding Claim 24, the combined system of Andersson and Oka discloses all claimed limitation as set forth above in claim 1. Further, Andersson discloses the wireless mobile communication station is pre-configured to only accept pushed packet data transmission from one or more originators in possession of certain predefined network address (see FIG. 4, step 174; see col. 6, line 5-14; see col. 8, line 3-65; see col. 9, line 35-40; mobile device is preconfigured/predefined to verify and accept the origination sources if received identifier/address of the origination source corresponds/matches the in-possession/stored identifier (i.e. user can only select/verify "the identifier" if the received identify matches/corresponds with stored/predetermined identifier). Oka also discloses the wireless mobile communication station is pre-configured to only accept pushed packet data transmission from one or more originators in possession of certain predefined network address (see FIG. 3-4, step S23-24, S33-S34; see col. 6, line 44 to col. 7, line 10, 30-40; see col. 8, line 3-11; mobile station is preconfigured/predefined/programmed to accept the call only received IDs and number matches the memorized IDs and number).

7. Claims 2 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andersson in view of Oka as applied to claims 1 and 13 above, and further in view of Lager (US006636502B1).

Regarding Claims 2 and 14, the combined system of Andersson and Oka discloses wherein each of said predefined network addresses of said set is associated, within the wireless communication station, with a name of originator (Andersson, see FIG. 4, step 172; see col. 6, line 4-10; see col. 7, line 60 to col. 8, line 2, 59-65; see col. 9, line 32-35; see col. 10, line 50-56;

identify of the origination source) from which it is desired to receive packet data as set forth above.

Neither Andersson nor Oka explicitly discloses a name of a network server. However, Lager discloses wherein each of said predefined network addresses of said set is associated (see FIG. 8, NIP-MEM stores a plurality of network indication), within the wireless communication station (see FIG. 8, GPRS-MS), with a name of a network server (see FIG. 8, ISP 1, ISP2, or ISP 3) from which it is desired to receive packet data (see col. 12, line 30-50).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide associating network address/indication with a name of ISP, as taught by Lager, in the combined system of Andersson and Oka, so that it would allow a subscriber a more flexible use of several external network servers; see Lager col. 8, line 55-60.

8. Claims 3, 4, 8, 15, 16 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andersson in view of Oka as applied to claims 1 and 13 above, and further in view of Wang (US006614774B1).

Regarding Claims 3 and 15, the combined system of Andersson and Oka discloses establishing a packet data session; determining whether or not the network address is authentic as set forth above in claims 1 and 13.

Neither Andersson nor Oka explicitly discloses an address translation server; requesting translation of the network address to a corresponding name of a network server; and determining based upon the result of said translation.

However, Lager discloses establishing a packet data session (see FIG. 4, IP session from host 130) with an address translation server (see FIG. 4, DNS server 118);

requesting translation of the network address to a corresponding name of a network server (see col. 8, line 32-47; reverse DNS lookups (i.e. from network address to the name of the server); and determining and connecting based upon the result of said translation (see col. 8, line 46-55; determine and connection utilizing result of reverse DNS lookups).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide a DNS server and reverse DNS lookups, as taught by Wang in the combine system of Andersson and Oka, so that it would avoid DNS lookup failures and does not introduce delays and cost effective system; see Wang col. 5, line 50-60.

Regarding Claims 4 and 16, Andersson discloses determine the network originator name with a previously stored network originator name the stored name being stored by the wireless communication station in such way that it is associated with the predefined network address matching said received network address (see FIG. 4, step 172; see col. 6, line 4-10; see col. 7, line 60 to col. 8, line 2, 59-65; see col. 9, line 32-35; see col. 10, line 50-56; mobile terminal must determine the received identifier/OA of the origination source associates/matches with stored/predetermined identifier/OA). Oka discloses comparing the network originator name with a previously stored network originator name the stored name being stored by the wireless communication station in such way that it is associated with the predefined network address matching said received network address (see FIG. 2, comparing unit 111; see FIG. 3-4, step S23-24, S33-S34; see col. 6, line 44 to col. 7, line 10, 30-40; see col. 8, line 3-11; the callee mobile station compares IDs and number of the caller mobile station if received IDs and number of the caller corresponds/matches the memorized IDs and number). Wang discloses the network server name returned by said address translation server as set forth above in claim 3.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide a DNS server and reverse DNS lookups, as taught by Wang in the combine system of Andersson and Oka, for the same motivation as set forth above in claim 3.

Regarding Claims 8 and 20, the combined system of Andersson and Oka discloses establishing a packet data session using the name of the network server as set forth above in claims 1 and 13. Wang discloses establishing a packet data session using the name of the network server, which name is returned by the translation server as set forth above in claim 3 and 15. Thus, the combined system of Andersson, Oka and Wang discloses all claimed limitation.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide a DNS server and reverse DNS lookups, as taught by Wang in the combine system of Andersson and Oka, for the same motivation as set forth above in claim 3.

9. Claims 9 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andersson in view of Oka and Wang, and further in view of Brothers (US006822955B1).

Regarding Claim 9 and 21, Andersson discloses said identity is the originator name as set forth above claim 1 and 13, and a network server (see FIG. 1, SMS-C, VPMSC 44, or GPMSC 46). Neither Andersson, Oka, nor Wang explicitly discloses an Internet domain host name of a network server. However, Brothers teaches wherein said name of network server is an Internet domain host name of a network server (see FIG. 13, a server Internet domain host name, "Disney.com"). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide an Internet domain host name as said name of the network server, as taught by Brothers in the combined system of Andersson, Oka and Wang, so that it would provide full transparent IP mobility services for clients; see Brothers col. 1, line 60 to col. 2, line 5.

Allowable Subject Matter

10. **Claims 10 and 22** would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Response to Arguments

11. Applicant's arguments with respect to claims 1-9,11-21,23 and 24 have been considered but are moot in view of the new ground(s) of rejection.

Regarding claims 1-9,11-21,23 and 24, the applicant argued that, "...the cited references fails to disclose or suggest, a method in which all packet data pushed to a mobile communication station is transmitted by the originator only after the wireless mobile communication station determines that the packet data is desired...Andersson merely discloses that, with respect to the network address of the originator of packet data, the network address of the originator is used to merely to determined whether transmitted packet data should be delivered, but has no disclosure that the address is then used to establish a session with originator...if Oka were used to modify Andersson, the combination fails to disclose or suggest the wireless mobile station of Andersson using an address of the Internet Host to establish communication...Oka also fails, when combined with Andersson to disclose using any address, let alone an address of an originator, to establish a packet data session, or an originator transmitting packet data only after acceptance by the mobile station..." in pages 10-14

In response to applicant's argument, the examiner respectfully disagrees that with argument above since the combined system of Andersson and Oka discloses the applicant claimed invention.

Andersson discloses verifying at the wireless mobile communication station the identity of the originator when the received network address of the originator matches one predefined network addresses stored by the wireless mobile communication station (see FIG. 4, step 174; see col. 6, line 5-14; see col. 8, line 3-65; see col. 9, line 35-40; mobile user verifies/authenticates/permits/selects the identify of the origination sources when received identifier/address of the origination source corresponds/matches the stored identifier/addresses (i.e. user can only verify/authenticate/permit/select "the identifier/address" if the received identifier/address matches/corresponds with stored/predetermined identifiers/addresses)); after verifying the identify of the originator (see col. 6, line 1-12; see col. 8, line 28-65; after verifying/authenticating/permitting identify of the origination source), the wireless mobile communication station using the received network address of the originator to establish a packet data session with the originator only after the identity of the originator is verified (see FIG. 4, step 176; see col. 6, line 10-14; see col. 8, line 10-14, 60-67; see col. 9, line 40-44; the mobile station using the OA of the origination source by initiating registration procedure in order to establish an end-to-end packet session/connection with the origination source only after the identify of the origination source is verified/authenticated/permitted), such that all the packet data is transmitted from the originator (see FIG. 4, step 176; see col. 5, line 65 to col. 6, line 14; see col. 8, line 59 to col. 9, line 5; so that all the packet data, which is not a SMS message request/query/signaling packet, is transmitted from the origination source to the mobile station via a registered end-to-end connection) only after the wireless mobile communication station determines that the received network address is included in the set of one or more predetermined network address stored by the wireless mobile station (see FIG. 4, step 168,172,174; only after the mobile station detects/determines that received identifier/address of the origination source corresponds/matches the stored/predefined identifiers/addresses by the mobile station and permitting/selecting accepted identifier/address of the origination source; see col. 8, line 21-44, 50 to col. 9, line 5).

Oka discloses determining at the wireless mobile communication station if the received network address matches a predefined network address of the originator (see FIG. 3, S22-S24; see FIG. 4, S32-34; determining/checking at Mobile Station (callee) if the received fixed ID, variable ID and telephone number of caller mobile station) is included in a set of one or more predefined network addresses stored by the wireless mobile communication station (see FIG. 2, Mobile station 1 memorizes IDs and telephone numbers (i.e. group/set of network addresses) of other mobile stations, and comparing unit 111 compares the received IDs and numbers with stored IDs and number; see FIG. 3-4, S23,S24,S33,S34; see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40), the set of one or more predefined network address corresponding to one or more predefined originators of data (see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40; the memorized IDs and numbers relate/correspond to other mobile stations (caller)); verifying, at the wireless mobile communication station, the identify of the originator when the received network address of the originator matches one or more of the predefined network address stored by the wireless mobile communication station (see FIG. 3, S22-S24; see FIG. 4, S32-34; verifying/authenticating at the callee mobile station the identify ID of the caller when received network ID/address of the caller recognized/matches the memorized network IDs/numbers of caller mobile stations; see col. 5, line 35-40,45-55; see col. 6, line 44-55; see col. 7, line 30-40); after verifying the identify of the originator (see FIG. 3, S23-27,S17; see FIG. 4, S33-S38; after verifying/authenticating the ID of the caller mobile station), the wireless mobile communication station using the received network address of the originator to establish a session with the originator at the wireless mobile communication station only after the identity of the originator is verified as being authentic (see FIG. 3, S23-27,S17; see FIG. 4, S33-S38; establishing communication with the caller mobile station at the callee mobile station after the verifying that the caller station is authentic; see col. 6, line 44 to col. 7, line 10, 30-40; see col. 8, line 3-11) such that all the data is transmitted from the originator (see FIG. 3, S17 and see FIG. 4, S38; when communication is established all the data transmitted from the caller station and received by the callee mobile station; see col. 7, line 5-11; see col. 8, line 5-11) only after the wireless communication station determines that the received network address is included in the set of one or more predefined network address stored by the wireless mobile communication station (see FIG. 3-4, S17/S38 (establishing communication step) at the callee mobile station occurs only after S22-24/S33-S34 (determining and authentication/verification steps) which determine by comparing the received caller IDs and number with the memorized IDs and number by the callee mobile station; see col. 6, line 44 to col. 7, line 10, 30-40; see col. 8, line 3-11).

In addition, it is well known that the memory of mobile device stores telephone/call numbers/address so that it can perform a matching and determining who is calling (i.e. originator).

Thus, in view of the above, it clear that the combined system of Andersson and Oka discloses the applicant claimed invention.

Moreover, Andersson's SMS message received by the mobile station is not a data packet as argued by the applicant. SMS message is a request/query/signaling/control packet to obtain a permission from the mobile so before registering/establishing an end-to-end communication. Establishing an end-to-end packet data session occurs only after the user of mobile terminal 14 is desired or accepted to receive packet data from the Internet host as described in below by Andersson.

> When the SMS message indicating the originator of the packet data is received at the receiver circuitry 142, such identification is displayed upon the display element 144. A user of the mobile terminal determines, responsive to the displayed information, whether to permit transmission of the packet data to the mobile terminal 14. Selection of permission to receive the packet data is entered by way of the selector 146. **When permission is granted to transmit the packet data to the mobile terminal 14, the mobile terminal 14 registers to receive packet data. Thereafter, the packet data is routed to the mobile terminal**. (see Andersson col. 8, line 33-44)
>
> Then, and as indicated by the block 166, the identity of the sending station from which the packet data originates is determined. **An SMS message is formed which indicates the identity of the sending station.** The SMS message is sent, as indicated by the block 168, to the mobile receiving station.
>
> The SMS message is detected at the mobile receiving station, as indicated by the block 172. **Selection is then made, as indicated by the block 174, whether to accept transmission of the packet data originated by the sending station. And, the packet data is sent to the mobile receiving station, indicated by the block 176, if the transmission is accepted at the mobile receiving station.**
>
> Thereby, packet data is transmitted to the mobile terminal only with the permission of the mobile terminal. **Transmission of undesired, or otherwise unsolicited, packet data is selectably prevented at the mobile terminal by denying permission to transmit the**

> **packet data thereto.** The user of the mobile terminal is able to control, thereby, which packets of data are transmitted to the mobile terminal. (see Andersson col. 8, line 55 to col. 9, line 5). (Emphasis added)

In view of the above, it is clear that an end-to-end packet data transmission over permitted/accepted end-to-end session/connection between the mobile terminal and the sending station or originator host is established only after the mobile station is accepted the transmission.

In response to argument, claim 23 does not recite, "**all** data packet" are transmitted from the originator only after the wireless mobile communication station determination. Thus, arguments on Andersson not disclosing "all" is irrelevant since the argued limitation are not being claimed. It is noted that the features upon which applicant relies (i.e., **all**) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Even if it were claimed, Oka discloses clearly discloses in FIG. 3 and 4 that "**all** packets" are transmitted from the originator only after the wireless mobile communication station determination to accept the call connection as set forth in responses above.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

In response to applicant's argument, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., an address of the **Internet** Host) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ian N. Moore whose telephone number is 571-272-3085. The examiner can normally be reached on 9:00 AM- 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Doris To can be reached on 571-272-7629. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ian N. Moore
Art Unit 2616

12-18-07

DORIS H. TO
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600